

Amendments to the Specification:

Please amend without prejudice the Specification as follows:

Please amend the paragraph beginning at line 34 of page 16 as follows:

--As shown in the figure, the distributed digital signature generation apparatus [[1]] 2 includes a certain number of partial digital signature generation parts 13 and an integrated digital signature generation part 14.--.

Please insert the following paragraph beginning at line 23 of page 17 as follows:

--The “Pair Of Digital Document and Partial Digital Signature” 17 is shown in Figure 3.--.

Please insert the following paragraph beginning at line 16 of page 18 as follows:

--The “Digital Document With Additional Information” 18 and the “Pair Of Digital Document With Additional Information And Partial Digital Signature” 19 are shown in Figure 4.--.

Please amend the paragraph beginning at line 8 of page 21 as follows:

--In the configuration shown in Figs. 2 and 3, each partial digital signature part 13i calculates $S_i(M) = H(M)^{D(i)} \bmod N$ ($1 \leq i \leq r$) for the input digital document M by using a proper hash function (for example, SHA-1 and MD5) whose range is included in $\{0, 1, \dots, N-1\}$. $S_i(M)$ is defined as a partial digital signature 16 for M.--.

Please amend the paragraph beginning at line 8 of page 27 as follows:

--As shown in Fig. 6, m subsets $I(0), \dots, I(m-1)$ of $\{r(1), \dots, r(m)\}$ are selected such that each $I(i)$ consisting of k elements and $I(i) = \{r(((j+i) \bmod m) + 1) \mid 0 \leq j \leq m-1\}$ ($i = 0, \dots, m-1$) in step 61.--.

Please amend the paragraph beginning at line 12 of page 27 as follows:

--The integrated digital signature $S(M', I(i))$ is generated from $\{S_{r(j)}(M') \mid r(j) \notin I(i)\}$ for each $I(i)$ ($i = 0, \dots, m-1$) in step 62.--.

Please insert the following paragraph beginning at line 19 of page 27 as follows:

--The next step 64 of Figure 7 is performed as follows:--.